Flexible Controls for Compliance in Catastrophe Management Processes

Kai Kittel
Stefan Sackmann

Veröffentlicht in:
Multikonferenz Wirtschaftsinformatik 2012
Tagungsband der MKWI 2012
Hrsg.: Dirk Christian Mattfeld; Susanne Robra-Bissantz

Braunschweig: Institut für Wirtschaftsinformatik, 2012

Flexible Controls for Compliance in Catastrophe Management Processes

Kai Kittel and Stefan Sackmann

Martin-Luther-Universität Halle-Wittenberg, Institut für Wirtschaftsinformatik und OR, 06108 Halle, E-Mail: { kai.kittel | stefan.sackmann }@wiwi.uni-halle.de

Abstract

Managing business processes is becoming increasingly flexible on both the conceptual and the technical level. Flexibility opens up new scopes of application. This contribution focuses on improving resilience of basic services (e.g., water supply) and rescue processes (e.g., firefighting) for catastrophic events by BPM approaches. However, flexibility is only seen as a necessary, but not sufficient condition for managing catastrophic events efficiently. Moreover, process flexibility has to be accompanied by comprehensive access to and processing of public as well as private information. Therefore, validating compliance is a still disregarded but crucial aspect. In this contribution, a model-based approach aiming at an automated adaptation of controls to changes of flexible processes is presented and discussed. As result, a future research agenda with concrete research topics is determined.

1 Flexibility and Compliance – Precondition for Effective Catastrophe Management Processes

Economic conditions and competition force many companies to continually search for ways to increase the efficiency of their (internal) operations [43]. Thus, a significant majority of companies use information and communication technology (IT) to support and execute their business processes and workflow management systems (WFMS) have been common practice for many years [39]. Increasing need for fast and efficient adaptation to changing demands from markets or customers' individual wishes keeps flexibility of business processes on the top of the agenda of many companies.

The need for flexibility is also an obvious topic for the management of catastrophic events. Typically, a lot of unforeseeable situations appear and flexible adaptation of ongoing catastrophe management processes (CM processes) to new situations and demands, such as maintaining basic services and rescue processes, is necessary and challenging [25], [28]. Apart from flexibility, a second important characteristic of any CM process is the validation of compliance with given rules and laws. At first glance, compliance might not be recognized as a necessary precondition for CM processes, since in the case of a catastrophic event (e.g., a destructive earthquake), staying compliant is unimportant when lives are at stake.

However, thinking of CM processes provided with flexible and comprehensive access to (sensitive) data, services and infrastructures also opens up enormous unforeseen opportunities in non-catastrophic situations, e.g., for surveillance, espionage, or intrusion into privacy. As discussed in more detail in [17], such an enormous potential of misuse could be expected to trigger a lot of social discussion and resistance, as happened with current approaches in automating data collection, integration, and analyses (e.g., SWIFT, e-Identity, RFID, or Google Street View [41], [48], [19]). Therefore, threats might be seen outweighing social benefits. Thus, powerful institutions that manage catastrophic events effectively could be expected not to gain acceptance in any open and free society. Apart from public reservations and resistance, it is doubtful that companies or private persons would cooperate on an individual level by providing free access to their data voluntarily without adequate "guarantees" and effective controls for compliance.

In this contribution, an approach for flexible integration of controls into processes is presented aiming at both the need for restrictive controls in the case of non-catastrophic events and the required flexibility of CM processes in the case of catastrophic events. For modeling information systems for catastrophe management, the conceptual separation of controls and (business) processes is discussed as a promising approach. The independent modeling of controls and business processes allows their flexible, context- and instance-specific integration on a model-based method. This contribution is completed by a detailed outline for a future research agenda and a short conclusion. Since research in this area is at very early stage, the focus lies on the identification of research problems and no evaluated artifacts are presented yet. However, the results of this paper already provide a sketch and an agenda for building research artifacts, thus laying the necessary foundation for future research in this field following the design-science paradigm [15].

2 Process Flexibility

Methods and tools for providing flexibility in process execution have been already developed and tested in the context of BPM (e.g., [30]). Research results show that process flexibility has to be tackled on two levels at least: firstly, on the conceptual level of the process itself and, secondly, on the operational level performing the activities. Flexibility on the conceptual level mainly addresses the capability to alter or extend the sequence of activities as well as the allocation of resources according to changed terms and conditions, e.g., to integrate (real-time) information or additional activities into instances of processes [33]. First methods and tools for providing flexibility at this conceptual level have already been developed and tested (e.g., [30]). Flexibility on the operational level mainly addresses the execution and support of activities with required and available IT infrastructure.

Currently, the most promising and common approach to gain flexibility on both levels are so-called service-oriented architectures (SOA). SOA provide a dynamic coupling of business processes with their underlying IT services (e.g., [18]) and, thus, to decouple business processes from their actual execution (e.g., [21]). The standardization of web service interfaces (e.g., [31]) allows IT services to be quickly changed technically and web services to be integrated/bought by third parties or provide/sell their own services [26]. If required, every instance of a workflow can be executed by different web services according to the actual execution environment [38] without needing changes on the conceptual process level.

In BPM, such ad hoc changes have so far often been seen as exceptions that are handled "manually". Typically, BPM in companies usually needs days or weeks for a structural adaptation of business processes, which cannot be accepted in catastrophe management situations. However, transferring the principles of BPM and SOA with their increasing support of information and flexibility to CM processes is very promising (e.g., [34], [16], [17]): on the one hand, the diffusion of BPM and web services in companies means a sound technical basis for integrating any kind of information and service into a CM process. Further progress is to be expected, since many companies already follow extensive integration strategies, for example IBM with its vision of a "smart planet" [13]. By representing real objects (with their characteristics and status) as services, they can be flexibly integrated into CM processes even "on the fly" [46]. For instance, if water supply over the communal water network breaks down or is constricted, supply could be realized, for example, with tank trucks or the distribution of bottled water. To integrate such alternative infrastructures efficiently into the management of CM processes requires additional real-time information about current storage capacities or transportation facilities that could be provided, for example by readily available services from companies that run tank trucks or beverage manufacturers. Relying on interlinked and distributed data sources can undoubtedly improve the MC processes.

3 Achieving Compliance by Flexible Controls

As discussed above, a flexible adaptation of CM processes by BPM approaches and comprehensive data access and usage by SOA is not a sufficient condition for realizing effective CM processes. A further crucial aspect is the ability to check and validate compliance of CM processes with regard to their usage of data and services.

Achieving transparency and validating compliance has already been a well-known challenge for many companies and their IT governance for several years (e.g., [49], [3]). Validating the adherence to and the fulfillment of various regulations (e.g., the Sarbanes Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), or the German Freedom of Information Act) when executing business processes has been one of the main issues of BPM. First research approaches for integrating a risk view into business process models can be found in so-called risk aware business processes (e.g.. [32], [50]). The annotation of risks in process models can at least give hints for possible misuse scenarios. While this might work for well-defined business processes, it is not sufficient for controlling emergency cases, not to mention for preventing any misuse. However, the conflict between compliance and "ad hoc" flexibility is not addressed in current business process approaches. Therefore, this section discusses current approaches addressing compliance breaches from both a classical IT security view and a BPM monitoring view. Extending the discussion in [17], it is shown that flexibility of the processes also requires flexibility of controls that is currently not yet achievable and opens a promising research field, not only for improving catastrophe management but also for supporting automation of companies' compliance in the future.

A basic foundation for validating compliant use of data and services is provided by "classical" IT security mechanisms. Mechanisms following an IT security approach for internet-based IT infrastructures means the adherence to protection goals (e.g., [22], [24]) that can result from laws, contracts, service usage conditions, etc. Available security mechanisms or

services assume that a data object has to be protected from unauthorized access. These mechanisms can be extended for usage control by complementing the conditions for data access by so-called obligations [29], i.e., rules having to be adhered to during process execution. For expressing compliance conditions and obligations in a formal manner, so-called policy languages have been developed (e.g., [10], [20]) and analyzed in the context of business process management [36]. Furthermore, advanced policy languages allow the comparison of different rules and the detection of contradictions [37]. This provides a technical basis for usage control by allowing the comparison of different specifications from various services provided, e.g., by companies. However, a practical implementation of such policy approaches lacks standardization, since policies are interrelated to the data as well as the specification and protocols for finding and communicating relevant policies. Although overcoming this obstacle is an important topic for providing emergency institutions with the required information, it is seen as part of future research and not yet addressed in this contribution.

The research in the area of business process compliance can therefore be summarized and clustered into three categories of controls differing in their restrictiveness to the underlying business process and the probability (and risk) of non-compliance (e.g., [37], [24], [9]):

- Compliance can be achieved “by design” [40], for example by redesigning the business process itself according to the laws. Alternatively, when designing business processes, the original process can be extended with additional control activities preventing any non-compliant execution. The enforcement of compliance can then be supported by automated WFMS guaranteeing the execution of the process as intended.
- Compliance can be achieved “during execution”, for example by analyzing the business process execution according to its coherence with policy or business rules. While compliance to formal specified access rules can be enforced by classical security monitors during runtime (e.g., [44]), compliance to formal specified usage rules (obligations) can at least be observed [23].
- Last but not least, compliance can be validated “by detection” [5]. Mechanisms for detecting non-compliance with policy rules are already available, e.g., secure logging files [1] or forensics [2]. However, these mechanisms are not capable of preventing any misuse; in the best case they allow, e.g., the starting of additional processes for palliating or the sanctioning of detected misuse non-technically [35].

As discussed, from a pure technical point of view, there are no mechanisms available that prevent any misuse with certainty. In practice, companies are forced to transparency, to change their processes, or at least to protocol whether breaches of regulations have happened for validating compliance with regulations ([47], [27]). Since the situation of catastrophe management institutions in non-catastrophic situations is more or less equal to the one of companies, a rigid compliance enforcement provided “by design” or “during execution” is wanted. The situation changes drastically in the case of a catastrophic event where the situation apparently differs from the one of companies: missing flexibility is seen as a significant disadvantage [8] and an unexpected and unintended halt of any CM process might interfere or disturb the originally intended CM process. This might mean, in the best case, only a conflict with the aims of effectiveness, in the worst case, it could endanger human life directly or indirectly. The conflict between enforcing compliant execution of

CM processes and the flexible adaptation to new and unforeseeable situations is obvious: while a rigid compliance enforcement provided “by design” or “during execution” is wanted and helpful from the policy side, it is not applicable in the case of catastrophe management. This leads towards a dilemma: since CM processes are usually difficult to predict, approaches preventing misuse “by design” or by halting the process “during execution” are very limited in their applicability to CM processes. On the other hand, control approaches that are capable of detecting misuse afterwards keep CM processes very flexible and, thus, seem to be more appropriate. However, their capability to prevent non-compliance and to reduce the risk of misuse is very limited. Solving this dilemma on a general level seems impossible. Therefore, our approach presented and discussed in the next section aims at a model-based adaptation of control activities in processes supporting both flexibility and validation of compliance.

4 Supporting Flexibility and Compliance in Catastrophe Management Processes

The main challenge to satisfying both the need for flexibility and the compliance to policy rules is the integration of control activities into CM processes during execution without disturbing them. The development of new methods and tools for changing business processes “on the fly” according to actual environmental conditions and without violating compliance requirements is an emerging field of research. The basic idea of our approach is to develop so-called control cascades that provide a methodic basis for identifying and adapting effective control activities on the level of individual instances of processes. Furthermore, advanced measures to determine the effects of control activities on the actually intended CM process are defined that allow skipping single controls if necessary, without losing controllability on a general level.

The model-based approach presented includes three main areas: firstly, the definition of reference controls that reflect a way control activities can be executed. Secondly, control cascades as a concept for modeling alternative control processes and their flexible integration into business/CM processes, and thirdly, an approach for integrating control activities into CM processes “on the fly”. The method provides first research results in the field, providing an improved adherence to compliance policies by integrating control activities as much as possible without disturbing the flexible execution of the actually intended CM process.

4.1 Modeling Reference Controls

Generic starting point for a methodic integration of control activities into business processes is the definition of (formal) compliance requirements. These requirements lead to (formal) rules reflecting the way how a company or institution wants to fulfill the relevant laws and regulations. In [6], a framework for transferring laws into such rules is given. For becoming part of any compliance management, a compliance requirement that is defined as relevant for the business process in mind has to be auditable, i.e., there has to be a mechanism to detect and to decide whether an executed business process adhered to the requirement or not. The validation is seen as core of compliance (e.g., [7]) and usually has to be proven to, e.g., external auditors or other investigators.

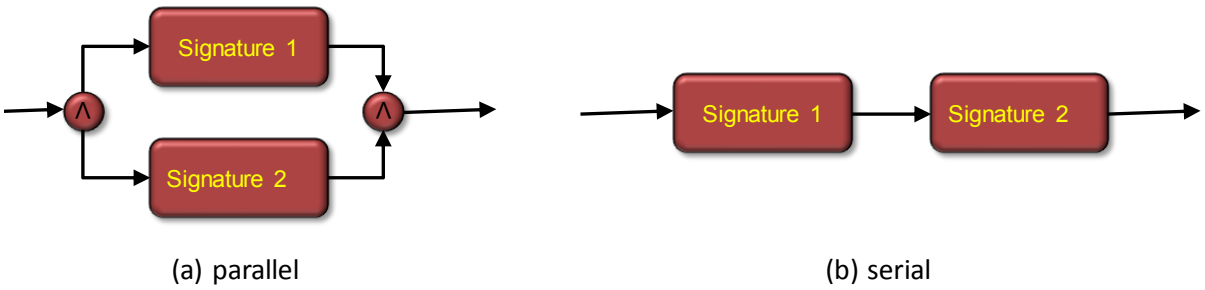

Figure 1: Examples for Reference Controls (Four-Eyes-Principle)

Since not all business processes and the distributed operators involved can be taken for granted to be compliant, several control activities are usually integrated into the business process (see the categories of controls in section 3). As described in [4], rules define which activities should or should not happen, for example activity B has to proceed after activity A is performed and, if control activities are efficient, in the best case, an auditor has nothing to complain about afterwards. For instance, the “second set of eyes” principle (compliance requirement) can be performed in a sequential or parallel way (see Figure 1), and it can be performed executing two activities straight consecutively or with other activities between (control activities). Each of these possible patterns can be modeled and represented by so-called reference controls. After the reference controls are defined and interlinked with the compliance requirement, the selection of appropriate controls and their integration into the business process are the next consecutive steps.

4.2 Control Cascades – Flexible Integration of Control and Business Processes

Each compliance requirement can usually be achieved by several different reference controls or control activities. For example, controlling the quality of water can be controlled by the water supplier at different points of the process, e.g., by analyzing the water sources, the water depots, or the hand-over to the consumer or by the consumer himself or herself. Each of these control activities can be of different types again, differing in efficiency and cost involved. Furthermore, control activities can be combined to achieve a satisfying control situation. Thus, the decision as to which control activities shall be actually integrated and at which point of a process is an open research question in the field of economics of controls [35]. While this decision has to be taken once in the case of more or less static processes, it becomes complex and challenging when the dynamic of the process is increasing and process activities as well as the executing entities are subject to unforeseen changes. When addressing dynamic CM processes, changing the process, for example by skipping activities or by changing the performing services and resources, can also effect control activities and, thus, make them unintentionally ineffective. To stay in control, a methodical approach as well as an automation of compliance is required. As discussed in [35], the separation of control and process models is a promising next step to automating compliance. By current “by design” approaches that interweave business process activities and control activities in one single model [42], a separated view on control activities on different levels of the process model is not achievable.

The fundamental concept for modeling controls in a process proposed in this contribution are so-called control cascades: their basic idea is not only to model the single control activity that is intended for achieving a compliance requirement but also to identify (all) alternative possibilities for integration (e.g,. earlier in the process). Furthermore, alternative control activities/ types are modeled that would address the same compliance requirement. Thus, control cascades are aimed at a model-based overview of known and available controls that could be implemented and combined to achieve a compliance requirement. The model serves for integrating necessary controls when changing the original process by (a) skipping activities or outsourcing a part of the process to external services, by (b) identifying controls that are no longer active, by (c) providing alternative controls and points for their integration into the changed process, and by (d) finding controls in the process which are still possible if an intended control activity is skipped. This allows improvement of the adherence to compliance requirements for flexible business processes too. For realizing such control cascades, however, the fundamental concept has to be substantiated.

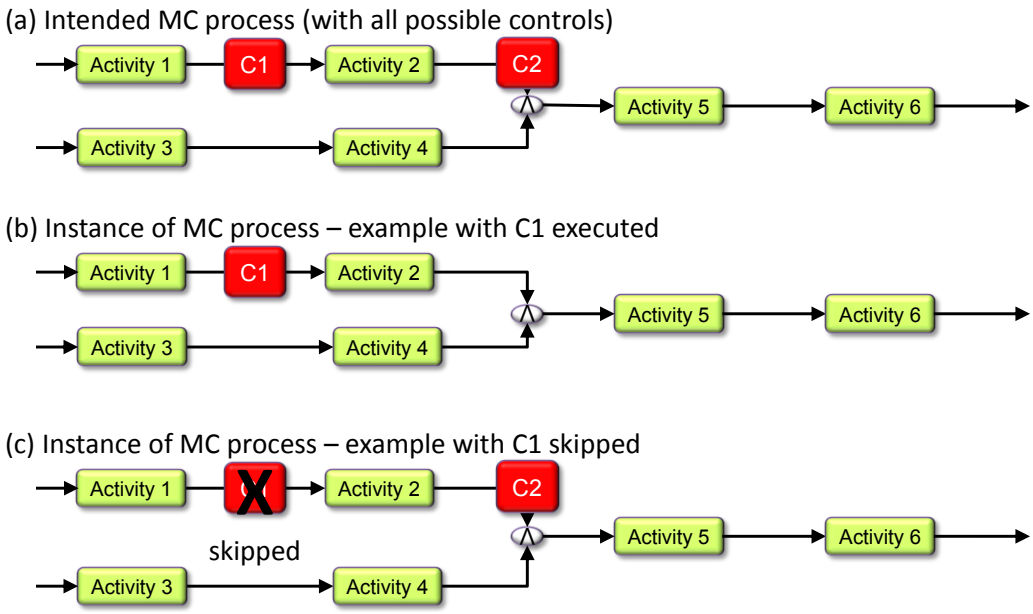

Figure 2: Example for Control Cascades

4.3 Integrating Controls into CM Processes “on the fly”

A flexible integration of reference controls in the form of concrete control activities into CM processes at the moment of process instantiation or during the process execution (see Figure 3) has a significant advantage: there are more pieces of information available than at design time, for example the number of people waiting for water or road condition for truck delivery. Such information should be used for adapting the CM process and the control activities to the real process context, for instance to implement control activities for testing water for nuclear radiation or a bactericidal contamination. Furthermore, the integration “on the fly” allows control activities to be skipped whenever the CM process is endangered by them. In this case, according to the control cascade approach, a further control activity supporting the same compliance requirement could be implemented automatically in the later process or the resultant compliance breach can be logged and evaluated later on.

To take all these criteria into account, information like inputs, outputs or the timeframe, which define the setting for the control activities, have to adhere. As described in [12], there are points in time during which control activities are alive, for example only if water information is needed and accessed do the water suppliers have to be informed. To achieve this requirement, validity period, activities as precondition, and/or activities as postcondition have to be defined and saved as additional information to the reference controls. Using all these pieces of information makes it possible to identify alternative points for defining control cascades as well as for integrating concrete control activities into a CM process by the help of automated search algorithms. Since there might be many points for integration theoretically possible, a reduction to efficient control points can be achieved by known methods already used by companies for many years, for instance by path analytics calculating the so-called critical path [47]. While in CM processes time matters particularly, other methods for cycle times, error ratios, or process costs can also be used in addition for achieving an effective selection of connection points for controls. By simulating the execution of the relevant process and by calculating different workflow scenarios, activity paths can be optimized and, thus, low-grade activities can be transferred into uncritical areas [14].

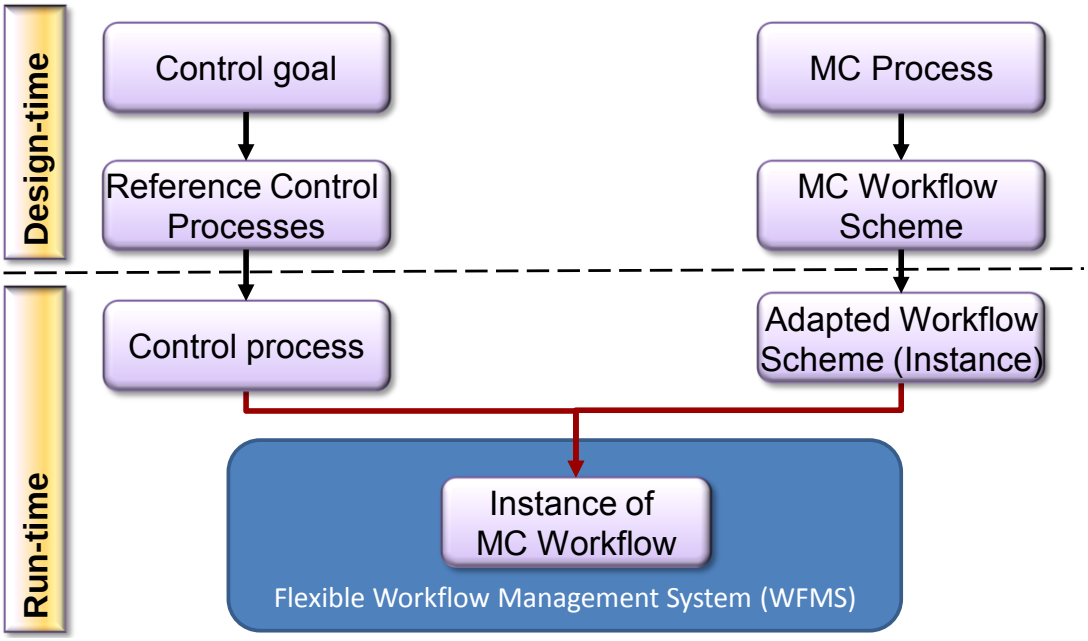

Figure 3: General Approach for Integrating Controls into MC processes "on the fly"

4.4 Open Research Questions

This contribution focuses on the compliance and control view of flexible CM processes that is neither taken into consideration adequately nor solved in current BPM approaches. The definition of reference controls and their transformation in control activities, the development of control cascades for selecting adequate control activities, and the integration of control activities into CM processes "on the fly" presented as new approach for improving catastrophe management by BPM methods and tools are still a draft and on an abstract level. However, the discussion already reveals some interesting topics for future research that are proposed as a future research agenda:

- Realizing the required IT infrastructure and integration is still challenging on the technical level: a central and powerful catastrophe management institution that could access whatever data and service needed would require a common semantic basis, which is not available yet. In BPM, cooperation usually is built on bilateral agreements to semantic business process models. This might not be practical for emergency institutions since too many actors and models are expected to be involved in CM processes. Thus, finding a common standard or advanced methods for bringing together different business process models is necessary and already object of current research (e.g., [45], [11]).
- Finding available services after a catastrophic event: To execute a CM process, activities have to be realized by those services and within those infrastructures that are still available in the case of a catastrophic event. Therefore, a way has to be found to detect services in an automatic manner, which is a current research topic in SOA research [18], [21]. Current approaches from BPM can possibly be adapted to catastrophic management situations, however, taking the special context explained above has to be taken into consideration and existing approaches have to be evaluated accordingly.
- Standardization of policy transmission: Current policy approaches lack standardization and therefore the practical implementation, especially concerning the specification and protocols for finding and communicating relevant policies, remains an open research topic. Overcoming this obstacle is important for providing catastrophe management institutions with the required information, since policies are interrelated to the data, which might be collected from different actors and processed by different web services.
- The optimal selection of controls: Since compliance requirements can be achieved in many different ways and by many alternative control activities, the relevant characteristics have to be measured. Since controls can be different in many ways, e.g., by their effectiveness, possibilities of circumvention, or costs, adequate ways to measure these characteristics and methods to find an optimal selection of control activities opens a challenging research field.
- Therefore, new methods of analysis are needed, e.g., extended critical path analysis, which also take into account the availability of non-technical services. Calculating critical paths requires predefined activities and assessable times of duration, which are hard to get in emergency situations. Staying with the example of water supply, for instance even if tank trucks are available, the time needed for delivery depends on the condition of the roads, which is barely predictable for earthquakes. Thus, for optimizing the effectiveness of CM processes, new ways for simulation and prediction are required. Furthermore, ways of identifying process and service vulnerabilities have to be found that allow the effect of changing activity sequences or availability of services to be calculated with respect to the effectiveness of the ongoing CM process.

5 Conclusion

Catastrophe management processes are mainly challenged by achieving both flexibility and compliance. In this contribution, successful methods and tools known from business process management are discussed as starting point for improving CM processes. However, since business processes and catastrophe management processes differ in their characteristics and specifications, a novel method to support the applicability of BPM approaches in an

emergency context is presented. While first results are very promising, it is also obvious that there are several hurdles to be overcome before a catastrophe management institution can realize all options of modern IT. The hurdles are not solely of a technical nature but also challenging from a social point of view. The main results of our analysis are:

- The underlying models, methods, tools, and infrastructure of business process management have obviously enormous capacity to support and improve CM processes. While the techniques of business process modeling can be used at the conceptual level, SOA as well as the standardization of web services can provide flexibility at the technical level. The main gap identified is to provide CM processes with flexibility on different levels not known in the typical business context without annulling compliance. To address this gap, a novel approach and research agenda for integrating controls flexibly into CM processes and, thus, for gaining flexibility in a catastrophic event situation by skipping control activities is presented. The results as well as the identified research questions do not aim at generating “pure” technical security for achieving compliance but at reducing the probability of misuse. Thus, the method provides a basis for a social discussion on endowing catastrophe management institutions with the required comprehensive and powerful access to data, processes, and services in the case of a catastrophic event.
- Further discussion of standardization on a technical level is seen as a precondition to support CM processes effectively by BPM methods and tools. Policies as well as context information need to be transferable and are not provided by pure web services interfaces today.
- Finally, the acceptable level of risk for CM processes is (and will remain) the subject of social and cultural discussion. However, by combining classical IT security solutions with the presented approach to stay flexible, at least the probability of compliance breaches and misuse is expected to be reduced significantly. In summary, the idea to integrate controls and processes at the time of instantiation seems to be a good starting point for gaining compliance for CM processes, although several aspects are still unsolved, indicating a promising future research agenda.

6 Literature

[1] Accorsi, R. (2009): Log Data as Digital Evidence: What Secure Logging Protocols Have to Offer? In: *Proceedings of the 1st IEEE Workshop on Computer Forensics in Software Engineering.* Seattle, Washington, USA.

[2] Accorsi, R.; Wonnemann, C. (2010): Static information flow analysis of workflow models. In: *Business Process and Service Science.* Leipzig, Germany.

[3] Arnold, V.; Benford, T.; Canada, J.; Sutton, S. G. (2008): The role of strategic enterprise risk management and organizational flexibility in easing new regulatory compliance. In: *International Conference on Enterprise Systems, Accounting and Logistics*, Crete, Greece.

[4] Awad, A.; Weske, M. (2010): Visualization of compliance violation in business process models. In: Rinderle-Ma, S., Sadiq, S. W., and Leymann, F. (Eds.), *Business Process Management Workshops*, Springer, Berlin.

[5] Brabänder, E.; Ochs, H. (2002): Analyse und Gestaltung prozessorientierter Risikomangementsysteme mit Ereignisgesteuerten Prozessketten. In: *Proceedings of GI-Workshop Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten*. Trier, Germany.

[6] Breaux, T. D. (2009): Legal requirements acquisition for the specification of legally compliant information systems, ProQuest, Ann Arbor, USA.

[7] Cannon, J.; Byers, M. (2006): Compliance deconstructed. ACMQueue, 4(7):30-37.

[8] Dadam, P.; Reichert, M.; Kuhn, K. (2000): Clinical Workfows - The Killer Application for Process-oriented Information Systems? In: *Proceedings of the BIS`00.* Poznan, Poland.

[9] Daniel, F.; Casati, F.; D'Andrea, V.; Mulo, E.; Zdun, U.; Dustdar, S.; Strauch, S.; Schumm, D.; Leymann, F.; Sebahi, S. (2009): Business compliance governance in service-oriented architectures. In: *Proceedings of the International Conference on Advanced Information Networking and Applications.* Bradford, UK.

[10] De Coi, J. L.; Olmedilla, D. (2008): A review of trust management, security and privacy policy languages. In: *Proceedings of the Int. Conf. on Security and Cryptography.* Porto, Portugal.

[11] Desai, N.; Mallya, A. U.; Chopra, A. K.; Singh, M. P. (2005): Interaction protocols as design abstractions for business processes. IEEE Transactions on Software Engineering, 31(12):1015-1027.

[12] Dwyer, M. B.; Avrunin, G. S.; Corbett, J. C. (1999): Patterns in property specifications for finite-state verification. In: *Proceedings of the 21st international conference on Software engineering,* Los Angeles, California, USA.

[13] Eckman, B.; Feblowitz, M.; Mayer, A.; Riabov, A. (2010): Toward an integrative software infrastructure for water management in the smarter planet. IBM Journal of Research and Development, 54(4):425-444.

[14] Flieder, K. (2006): Geschäftsprozessmanagement–Geschäftsprozesse mit dem virtuellen Reißbrett steuern. WING-business, 39(3):35-38.

[15] Hevner, A. R.; March, S. T.; Park, J.; Ram, S. (2004): Design science in information systems research. Mis Quarterly, 28(1):75-105.

[16] Jaeger, M. C.; Ladner, H. (2005): Improving the QoS of WS compositions based on redundant services. In: *Proceedings of the International Conference on Next Generation Web Services Practices (NWeSP).Seoul, Korea.*

[17] Kittel, K.; Sackmann, S. (2011): Gaining Flexibility and Compliance in Rescue Processes with BPM, In: *Proceedings of ARES Conference - Workshop on "Resilience and IT-Risk in Social Infrastructures" (RISI 2011),* Vienna, Austria.

[18] Krafzig, D.; Banke, K.; Slama, D. (2005): Enterprise SOA: service-oriented architecture best practices. Englewood Cliffs: Prentice Hall.

[19] Krys, C.; Wiedemann, A. (2011): Google – In Zukunft vergessen Sie nichts, weil der Computer sich alles merkt“. In: Bieger, T. et al. (Eds.), *Innovative Geschäftsmodelle. Konzeptionelle Grundlagen, Gestaltungsfelder und unternehmerische Praxis.* Springer, Berlin.

[20] Kumaraguru, P.; Cranor, L.; Lobo, J.; Calo, S. (2007): A survey of privacy policy languages. In: *Proceedings of the 3rd Symposium on Usable Privacy and Security.* Pittsburgh, USA.

[21] Melzer, I. (2010): Service-orientierte Architektur. In: Melzer, I. (Ed.), *Service-orientierte Architekturen mit Web Services.* Spektrum Akademischer Verlag.

[22] Müller, G.; Accorsi, R.; Höhn, S.; Kähmer, M.; Strasser, M. (2007): Sicherheit im Ubiquitous Computing: Schutz durch Gebote? In: Mattern, F. (Ed.), *Die Informatisierung des Alltags*, Springer, Berlin.

[23] Müller, G.; Accorsi, R.; Höhn, S.; Sackmann, S. (2010): Sichere Nutzungskontrolle für mehr Transparenz in Finanzmärkten. Informatik-Spektrum, 33(1):3-13.

[24] Namiri, K.; Stojanovic, N. (2007): Using control patterns in business processes compliance. In: Wekse, M. (Ed.), *Proceedings of the Workshop on Web Information Systems Engineering.* Nancy, France.

[25] Nell, M.; Richter, A. (2005): Catastrophic events as threats to society: Private and public risk management strategies. Risk Management, 321-340.

[26] Österle, H.; Reichmayr, C. (2006): Outtasking mit WebServices. In: Bullinger, H.-J. and Scheer, A.-W. (Eds.), *Service Engineering.* Springer Berlin, Heidelberg.

[27] Parker, C. (2003): Regulator Required Corporate Compliance Program Audits. Law & policy, 25(3):221-244.

[28] Pearce, L. (2003): Disaster management and community planning, and public participation: how to achieve sustainable hazard mitigation. Natural Hazards, 28(2): 211-228.

[29] Pretschner, A.; Hilty, M.; Schutz, F.; Schaefer, C.; Walter, T. (2008): Usage control enforcement: Present and future. Security & Privacy, IEEE, 6(4):44-53.

[30] Reichert, M.; Rinderle, S.; Kreher, U.; Dadam, P. (2005): Adaptive process management with ADEPT2. In: *Proceedings of the 21 th ICDE.* Tokyo, Japan.

[31] Richter, J. P.; Haller, H.; Schrey, P. (2005): Serviceorientierte Architektur. Informatik-Spektrum, 28(5):413-416.

[32] Rieke, T.; Winkelmann, A. (2008): Modellierung und Management von Risiken. Ein prozessorientierter Risikomanagement-Ansatz zur Identifikation und Behandlung von Risiken in Geschäftsprozessen. Wirtschaftsinformatik, 50(5):346-356.

[33] Rinderle, S.; Reichert, M.; Dadam, P. (2004): Correctness criteria for dynamic changes in workflow systems--a survey. Data & Knowledge Engineering, 50(1):9-34.

[34] Rose, T.; Peinel, G.; Arsenova, E. (2008): Process management support for emergency management procedures, eChallenges e-2008 Conference, Stockholm, Sweden.

[35] Sackmann, S. (2011): Economics of Controls. In: *Proceedings of the International Workshop on Information Systems for Social Innovation 2011 (ISSI 2011).* Tokyo, Japan.

[36] Sackmann, S.; Kähmer, M. (2008): ExPDT: A Policy-based Approach for Automating Compliance. Wirtschaftsinformatik, 50(5):366-374.

[37] Sackmann, S.; Kähmer, M.; Gilliot, M.; Lowis, L. (2008): A classification model for automating compliance. In: *Proceedings of the IEEE Conference on E-Commerce Technology (CEC'08).* Washington, USA.

[38] Sackmann, S.; Lowis, L.; Kittel, K. (2009): Selecting services in business process execution - a risk-based approach. In: Hansen, H. R. et al. (Eds.), *Business Services: Konzepte, Technologien, Anwendungen, Tagung Wirtschaftsinformatik (WI09).* Vienna, Austria.

[39] Sackmann, S.; Strüker, J. (2005): Electronic Commerce Enquete: 10 Jahre E-Commerce: Eine stille Revolution in deutschen Unternehmen. Konradin-IT-Verlag, Leinfelden.

[40] Sadiq, S.; Governatori, G.; Namiri, K. (2007): Modeling control objectives for business process compliance. Business Process Management, 149-164.

[41] Schaar, P. (2007): Das Ende der Privatsphäre. Wilhelm Goldmann Verlag, München.

[42] Schumm, D.; Leymann, F.; Ma, Z.; Scheibler, T.; Strauch, S. (2010): Integrating Compliance into Business Processes: Process Fragments as Reusable Compliance Controls. *Proceedings of the Multikonferenz Wirtschaftsinformatik (MKWI'10).* Göttingen, Germany.

[43] Smith, H.; Fingar, P. (2003): Business process management: the third wave. Meghan Kiffer Press, Tampa (FL), USA.

[44] Thomas, M.; Redmond, R.; Yoon, V.; Singh, R. (2005): A semantic approach to monitor business process. Communications of the ACM, 48(12):55-59.

[45] van der Aalst, W.; van Hee, K.; Massuthe, P.; Sidorova, N.; van der Werf, J. (2009): Compositional Service Trees Applications and Theory of Petri Nets. In: Franceschinis, G. and Wolf, K. (Eds.), Springer Berlin.

[46] van der Aalst, W.; van Hee, K. M. (2004): Workflow management: models, methods, and systems. The MIT press. Boston, USA.

[47] Verworn, B. (2003): Projektplanung während der frühen Phasen. In: Herstatt, C. and Verwom, B. (Eds.), *Management der frühen Innovationsphasen: Grundlagen - Methoden - neue Ansätze.* Gabler, Wiesbaden.

[48] Weber, M. (2009): Europäische Standards für den weltweiten Datenschutz. Zeitschrift für außen-und Sicherheitspolitik, 2(2):182-192.

[49] Weill, P.; Ross, J. W. (2004): IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press, Boston, USA.

[50] zur Muehlen, M.; Rosemann, M. (2005): Integrating risks in business process models. In: *Proceedings of the Australasian Conference on Information Systems.* Sydney, Australia.